National Domestic Communications Assistance Center (NDCAC)
Executive Advisory Board (EAB)
Report to the Attorney General

October 2017

National Domestic Communications Assistance Center (NDCAC)
Executive Advisory Board (EAB)
Report to the Attorney General

Table of Contents

National Domestic Communications Assistance Center (NDCAC)
Executive Advisory Board (EAB)
Report to the Attorney General

Executive Summary

Lawfully authorized electronic surveillance and digital forensics are vital tools for law enforcement to investigate criminals; gather evidence and intelligence; and protect national security. However, law enforcement is increasingly unable to access, intercept, collect, and process wire or electronic communications and stored communications information. Challenges such as the prevalence of end-to-end encryption, service mobility, anonymization, outdated statutes, and the lack of a mandate regarding data retention erode law enforcement's ability to obtain critical information that may be used to identify and save victims, reveal evidence to convict perpetrators, and/or exonerate the innocent. These challenges, when considered in totality, are referred to as "Going Dark" - the widening gap between law enforcement's court ordered authority to collect evidence and the ability to gain access to that evidence in a meaningful way.

The National Domestic Communications Assistance Center (NDCAC) was established by the Department of Justice (DOJ) as a national center for information sharing among members of the Federal, State, local, and tribal law enforcement community in part to assuage some of these challenges. An important aspect of the NDCAC is its Executive Advisory Board (EAB), a fifteen-member, State and local plus-one majority board composed of executive managers from across law enforcement. It is governed by the Federal Advisory Committee Act (FACA) and provides advice and recommendations to the Attorney General (or his designee) and to the Director of the NDCAC. This first report outlines five significant challenges facing the law enforcement community (i.e., technical challenges associated with electronic surveillance, communications evidence, and technical location capabilities; resource challenges that are particularly acute at the State, local, and tribal level; and statutory challenges that are the result of laws not keeping pace with the profound evolution of communications services and devices) and provides the Attorney General insight into the NDCAC and its constituent programs.

The NDCAC EAB also recognizes it must identify a path forward for it to better understand the short-term and long-term implications of the changing nature of crime as well as the rapid and ongoing communications transformation. The NDCAC EAB established a Technology Subcommittee to provide insight and an in-depth understanding to the EAB of the challenges faced by the law enforcement community which will allow it to more effectively advise the Attorney General. Additionally, a Technology Subcommittee furthers the EAB's overall mission to provide advice and guidance to the Director of the NDCAC through the identification and examination of potential NDCAC projects, tools, and training.

Introduction

Technological impediments to law enforcement's ability to exercise the authority granted to safeguard the public (through lawful access to communications, devices, and records) have been introduced periodically throughout our history. As a society, we have had to decide how to mitigate those technological impediments and ensure law enforcement's continued lawful access. One example of how the nation chose to mitigate technological impediments was with the enactment of the Communications Assistance for Law Enforcement Act (CALEA).[1] In October 1994, Congress acted to protect public safety and national security by enacting CALEA to clarify and further define existing statutory obligations of providers of telecommunications services in assisting law enforcement in executing electronic surveillance court orders. CALEA did not change or expand law enforcement's fundamental statutory authority to conduct various types of electronic surveillance. It sought to ensure that once law enforcement obtained the appropriate legal authority, telecommunications carriers would have the necessary technical capability to fulfill their statutory obligations to assist law enforcement. In the intervening 20 plus years since the passage of CALEA, law enforcement has seen the severe erosion of the capability to intercept communications because of rapid technological advances and profound shift in communications technologies in use today.

Law enforcement recognizes that network security measures such as encryption are important and supports efforts to use encryption and other technologies to secure cell phones, email, text messages, and other online communications and transactions. Further, law enforcement sees the need to identify methods to protect and ensure privacy and to do so in a transparent and open way while simultaneously ensuring its ability to protect the public safety and national security is not compromised.

Accomplishments of the EAB

The NDCAC EAB held its first meeting in September 2016 in accordance with the FACA. This introductory public meeting was intended to familiarize members with the functionality of the NDCAC as well as lay out a forward-looking agenda for the NDCAC EAB. The NDCAC EAB had established an Administrative Subcommittee to begin the important initial work of providing a framework under which the EAB would operate. To that end, the Administrative Subcommittee developed draft bylaws for the consideration of the full NDCAC EAB. The bylaws were discussed and approved during the NDCAC EAB's September meeting.

The NDCAC EAB Administrative Subcommittee also undertook the responsibility of developing a recommendation for an NDCAC Director for the NDCAC EAB's consideration. Over the course of months, the Administrative Subcommittee researched several potential avenues for the NDCAC EAB to recommend to the Attorney General a candidate to be the Director of the NDCAC. The Administrative Subcommittee concluded the then current Interim Director, Ms. Marybeth Paglino, was the best suited candidate to be the first Director of the NDCAC. In its recommendation to the full NDCAC EAB, the Administrative Subcommittee cited that Ms. Paglino had overseen the establishment of the NDCAC and guided its development from the drawing board to maturity; was an instrumental force in getting the NDCAC off the ground; and

[1] Pub. L. No. 103-414, 108 Stat. 4279

had long been an advocate for the NDCAC and its focus on the State and local law enforcement community. The Administrative Subcommittee recognized that as a former Federal Bureau of Investigation (FBI) Special Agent with more than thirty years of experience, Ms. Paglino understood the technical challenges faced by law enforcement and the realities of how communications services and devices impact investigations.

The NDCAC EAB Administrative Subcommittee also worked to identify candidates for the NDCAC Deputy Director position. Members of the Subcommittee recognized challenges associated with filling the position with an active member of the State and local law enforcement community and concluded that a candidate from the Drug Enforcement Administration (DEA) fill the NDCAC Deputy Director position. The Subcommittee will work with the DEA and identify candidates for the full NDCAC EAB to consider and recommend for appointment by the Attorney General.

Law Enforcement Community Challenges

One of the primary responsibilities of the NDCAC EAB is to provide advice to the Attorney General regarding: the technical challenges facing law enforcement agencies with respect to lawfully authorized electronic surveillance, collection of communications evidence, and technical location capabilities. These challenges are particularly acute for members of the State, local, and tribal law enforcement community. There have been numerous efforts to examine the issues faced by law enforcement. For example, the International Association of Chiefs of Police (IACP) organized a Law Enforcement Summit on Going Dark in February 2015. That Summit brought together a diverse group of law enforcement executives and investigators; privacy experts, legal specialists, scholars, and other professionals to explore the challenges faced by law enforcement and to examine the technical, operational, legal, and policy issues associated with these challenges. That Summit resulted in a report[2] that identifies the technological and legal landscape surrounding the issue of Going Dark and the barriers to access faced by all levels of law enforcement. The report also identifies a list of recommended strategies and action steps for pursuing balanced solutions to the issue of Going Dark.

Technical Challenge - Electronic Surveillance

The challenges surrounding electronic surveillance, or data in motion, are varied in nature, but the source of many of them is grounded in the fact that no mandate exists for entities that provide communications services to maintain any capabilities with which to comply with court ordered authorized law enforcement access. This is, in part, the result of the changing nature of the communications industry, the dramatically lower barriers to entry for non-facilities based providers, and a legislative and regulatory regime that has not kept pace.

Absent a mandate for access and the resulting technical solutions, law enforcement has little or no likelihood of insight into the information exchanged between the target(s) of an investigation and their associates. Today, that exchanged information could still often be accessed in an

[2] 2015 IACP Summit Report, "Data, Privacy, and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence."

unencrypted form by service providers if solutions were mandated. This also applies to the communications identifying information or metadata upon which many investigations rely.

Some providers with access solutions have chosen to utilize third party encryption to nullify law enforcement's comprehension of the communications that it can access. In those instances, law enforcement often foregoes pursuing a court order knowing that any communications it collects will be undecipherable. The plain text of transmitted information is critical in law enforcement investigations.

Further, the mobility or transferability of products and services within and between providers challenges the ability of law enforcement to identify and collect pertinent communications. The ability of targets to seamlessly utilize multiple devices, providers, and technologies to communicate makes it virtually impossible for law enforcement to identify, process, and analyze the communications and data in a meaningful manner.

Today's communications architecture also allows providers to offer service from beyond the reach of domestic law enforcement. Service providers can offer their products and services from outside the United States (U.S.), beyond the reach of law enforcement and U.S. courts, diminishing law enforcement's ability to serve legal process and access subjects' communications.

Technical Challenge - Communications Evidence

Records of various kinds of activity (e.g., communications, financial transactions) play a pivotal role in many investigations. Records of communications often form the foundation for establishing the probable cause for more intrusive methods of surveillance and establish the relationships between and among co-conspirators, assist in identifying individuals, reveal the scope of the criminal organization, and detail patterns of activity.

The evolution of communications services has also had a profound impact on the recordkeeping of service providers. In the past, records of communications were of paramount importance to service providers as they formed the basis upon which subscribers were billed for access to the network and for other services. That is often no longer true. There is little need for a service provider to keep records for a flat rate or unlimited usage service. For those service providers that do keep some records, there is no statutory guidance. Further, no uniform industry practice exists regarding records retention or the scope or format of those records. Inconsistent industry practices can lead to confusion and wasted law enforcement resources.

Information stored on subscriber devices is indispensable for law enforcement in the investigation and resolution of a wide range of crimes including but not limited to terrorism, child pornography, sexual abuse, narcotics trafficking, and gang violence. However, that crucial data is only useful if it can be accessed and deciphered. Manufacturers of consumer communications devices have recently instituted a default and compulsory capability by which all information stored on a device is automatically encrypted, and they have done so in a way to ensure that not even they can access the potential evidence. Further, manufacturers have taken the additional step of ensuring that law enforcement's attempts to access locked devices will result in the deletion of all evidence on the device after a limited number of attempts.

U.S.-based service providers are also increasingly storing records in foreign countries. The impact of storing records on foreign servers is significant as the use of a valuable investigative tool is becoming more limited. The only option available for law enforcement would be to seek evidence through mutual legal assistance treaties (MLAT). However, for those countries with which the U.S. has an MLAT, U.S. law enforcement requests must navigate often inefficient mechanisms to have the requested information transferred. In addition, MLAT agreements do not reach every country or cover all crimes which leaves law enforcement without any recourse to get critical evidence. The issue of where records are stored and how law enforcement may access them is also particularly acute with service providers that offer their products and services from outside the U.S.

Technical Challenge - Technical Location Capabilities

The ability to definitively ascertain the location of the subject of an investigation or the victim of a crime is fundamental to law enforcement's mission to protect the public. Understanding the communications infrastructure that supports service providers' ability to locate mobile devices and offer services and having that information available during investigations is critically important to law enforcement. When authorized to access it, law enforcement needs service providers to make available all reasonably available device and service location information available at the most granular level of detail possible.

However, there are instances where inconsistent practices impede law enforcement from gaining insight into the location of a subject of investigation or a victim of crime. For example, data that associates location with Internet Protocol (IP) addresses is not consistently specific or detailed enough for law enforcement purposes. At their least precise, IP addresses can be associated with the geographic centers of cities, states, or the entire country – tens, hundreds, or thousands of miles away from a specific user, device, or service.

Further, some forms of location information are often not available in the absence of the lawful authority to collect the content of communications. For example, many mobile devices include the time, date, and location data of photos taken by a user. This information is critical to law enforcement in a wide range of crimes such as kidnapping, child pornography, and child sexual abuse. However, there is no way for law enforcement to gain access to location information without collecting the content information – the digital image – for which law enforcement may not have sufficient probable cause for a court order.

Resource Challenge

Law enforcement, because of its diffuse nature and variety of policing responsibilities, has not been invested with the necessary infrastructure to ensure it maintains the necessary technological prowess to address the increasing number of technical challenges. Specifically, the State and local law enforcement community has been historically under-resourced with respect to the tools and technologies necessary to assuage the impacts of Going Dark.

Further, law enforcement's resource challenges have been exacerbated by the fact that the nature of crime itself has changed. The technical sophistication of criminals at the State and local level has risen dramatically. Criminals have historically made use of the services and technologies

generally available to society and as those have become increasingly sophisticated, they have had a disproportionate impact on the law enforcement community. For example, the introduction of default encryption, while lauded for its security benefits of protecting users' data, has a devastating impact on law enforcement attempts to collect evidence of a crime.

It is important to stress that any resources directed to law enforcement to address the technical challenges identified above cannot come at the expense of existing programs or other efforts. Augmenting law enforcement capabilities to address the challenges of a technological age cannot be a zero-sum game. While the establishment of the NDCAC is helpful and its impact widespread, it was never intended to address all the technical shortcomings within individual law enforcement agencies that often lack critically important expertise and the most up to date equipment. In short, the NDCAC represents an important aid, not a complete solution.

Statutory Challenge

The effectiveness of statutes designed to assist law enforcement are directly linked to the scope of their mandate. For example, at the time of CALEA's enactment, the portion of the communications infrastructure covered by the law was significant (i.e., landline and cellular telecommunications carriers). In 2005, the scope was expanded through a decision from the Federal Communications Commission (FCC) to include interconnected Voice over Internet Protocol (VoIP) service providers and providers of broadband Internet access services as, at the time, they were substantial replacements for traditional telephony.

However, the communication industry's migration away from traditional services has resulted in marginalizing CALEA's coverage of communication services (as enacted and as expanded by the FCC) utilized by the public. In fact, services and technologies considered too immature to be covered by CALEA during the debate preceding enactment have superseded the very telecommunications services thought to be the greatest threat to law enforcement's capability to conduct electronic surveillance at that time. Additionally, application-based electronic messaging, non-existent at the time of CALEA's enactment has matured to the point of near ubiquity that permeates every method of communications available today. Law enforcement now finds itself in a situation where it can be granted the authority by a court to intercept communications from a provider with no capability to carry out the authorized interception. However, modern communications providers not covered by the CALEA technical assistance capability mandate often render the orders moot.

The law has not kept pace with changing communications technology as an increasing number of relevant service providers fall outside the coverage of CALEA. Many popular Internet-based service providers are not required to maintain technical solutions for intercepting either communications or providing communications identifying information. When served with a court order to assist law enforcement in intercepting communications, providers not subject to the capability requirements imposed by CALEA are often unprepared and unwilling to comply. Even telecommunications providers that are required by law to maintain intercept solutions often do not. They are often slow at providing the technical assistance necessary to effectuate the surveillance, frequently taking weeks or months to provide a capability, which means that criminals have additional weeks or months to continue perpetrating their criminal schemes.

The increasing prevalence of the Internet and the introduction of services outside the scope of CALEA resulted in law enforcement's collection capability to drop significantly. Additionally, law enforcement's ability to collect evidence (data) at rest has been significantly reduced because of the increased variety and complexity of advanced services and technologies.

The law enforcement community is also concerned about recent renewed efforts to amend the Electronic Communications Privacy Act (ECPA). There have been numerous bills (e.g., H.R. 387), but none balance the needs of law enforcement with measures to protect privacy. Law enforcement has developed the following primary ECPA reform principles it believes need to be incorporated in any legislative amendment of the law.

- *Emergency Situations* - ECPA should allow service providers to be compelled to produce either communications content or records without a warrant in the event of an emergency or if the Government has the consent of the customer or subscriber.
- *Outdated Provisions of ECPA* - ECPA should reflect newer developments affecting law enforcement's ability to obtain evidence. For example, references to telephone calls within Section 2703 should be replaced with modern language more in line with modern electronic communications (e.g., "source and destination information").
- *Issues with Service Provider Responsiveness* - ECPA should address the real and widespread problem law enforcement has with service providers' lack of responsiveness, particularly when provisions are voluntary (e.g., in emergency circumstances, provider disclosures are voluntary and the provider determines whether an emergency exists).
- *Access to Records Held Outside the U.S.* - ECPA should address how law enforcement can access the evidence it needs when records are stored across a multinational network (i.e., stored abroad) and service providers insist on localized service of process.

Changing Nature of Crime

A dominant force of change in all our lives is how we use, interact, and are influenced by technology. Communications services and technologies have profound impacts on our social circle, access to information, and our perception of the world around us, making it smaller and effectively erasing borders that once seemed impermeable. Today, information is available instantaneously and anywhere one can gain access to a signal, be it paid broadband, cellular or free Wi-Fi. To the extent that such access benefits society, it should be embraced and encouraged to flourish. But there is a very real downside to this ubiquitous access, the misperception that the information is complete and therefore represents all possible data from which definitive conclusions can be drawn.

One area where this misperception is dangerously misleading is crime statistics. Simply stated, crime is not down, it is different. It is different, not only in the way it is committed in the continually evolving world of technology, which offers criminals a wide and varied source of new opportunities and techniques to commit crime, but it is also different from the picture it creates of the crime problem. The method of counting crime currently in use was developed in 1929. While it has been modified and broadened since that time, it still focuses on the public's concerns about crime as it existed nearly ninety years ago.

The Uniform Crime Reporting (UCR) Program collects data about Part I offenses (i.e., criminal homicide, forcible rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson) to measure crime occurring across the country. The rationale behind assessing these specific crimes is based on the fact that they are serious crimes, they occur with regularity in all areas of the country, and they are likely to be reported to police. Law enforcement agencies also report arrest data for 21 additional crime categories (i.e., Part II offenses).

However, for crimes that have a technological nexus or crimes that are more easily facilitated by the wide availability and increasing sophistication of communications technologies, there are likely few or no reliable statistics. There is no clear picture or understanding of the extent of crimes such as child sex trafficking, fraud against government resources, official corruption, or support of violent extremism. The occasional arrest is not sufficient to understand the depths of the issues associated with these crimes. And unlike the Part I offenses named above, the likelihood of a victim reporting them is low.

In short, our understanding of crime has changed. In totality, crime is markedly different. To be sure, the crimes for which statistics are collected by the UCR Program still occur with regularity, but the breadth and scope of crimes has expanded dramatically. The changing nature of crime necessitates a change in how law enforcement approaches its investigations of crime – better understanding of the communications services and technologies that are used in the furtherance of criminal activity; unearthing the information that may be available from providers; piecing together information from disparate sources; and gaining access to tools and techniques from within the nationwide law enforcement community.

Quantifying the Problem

The technological, resource, and statutory issues facing the law enforcement community, outlined above, are well understood by agencies and investigators. However, the interrelated and intersecting nature of the issues make it difficult to empirically quantify the number of investigations impacted. For example, investigators do not pursue electronic surveillance court orders if technical capabilities are not available from providers; in many cases, providers are not required to have considered law enforcement needs for their service or technology; and records that are no longer kept in the normal course of business and therefore cannot aid an investigation are not requested.

Notwithstanding the inherent difficulty in capturing information to enumerate the variety of impediments, several major national law enforcement and prosecutorial associations developed a Statistics Collection Tool to catalog investigatory impediments (i.e., electronic surveillance, records requests, and mobile devices) experienced by law enforcement. The NDCAC assisted in the associations' development of the Statistics Collection Tool to better quantify the full impact of "Going Dark" on investigations and cases and continues to facilitate the collection of data from participating agencies. The effort to collect statistical information is ongoing.

Participants in the effort have learned a great deal about the challenges associated with collecting the statistical information. Information pertaining to a diverse set of challenges cannot often be found within a single repository at an agency; multiple organizations within an agency may be

responsible for measuring different types of impediments. Further, participants are often unable to fully contribute because unsuccessful attempts to collect evidence are not uniformly documented. As the central aggregator of information, the NDCAC must try to resolve jurisdictional and agency-specific policies that result in an assorted dataset.

Establishment of NDCAC

The Department of Justice (DOJ) established the NDCAC as a national center for information sharing among members of the law enforcement community. Its formal mission is "to leverage and share the collective technical knowledge and resources of the law enforcement community on issues involving real-time and stored communications and to strengthen law enforcement's relationship with industry." The need for the NDCAC is the result of an ever more diverse and complex communications environment that adversely impacts law enforcement's ability to investigate criminal wrongdoing and protect the public safety. The NDCAC provides technical assistance to the law enforcement community; leverages individual agencies' research and development efforts for the greater benefit of the community; provides a mechanism to make solutions available throughout the community; provides training to raise the level of technical understanding and awareness within the law enforcement community; and establishes and maintains relationships with industry to better understand business and technology trends.

The FBI initiated the "Going Dark" discussion with other Federal, State, and local members of the law enforcement community over a decade ago. The first meeting, held in 2005, opened the dialogue that defined what needed to be addressed by a comprehensive, law enforcement-wide strategy to meet the needs of the *entire* law enforcement community. Representatives of Federal, State, and local agencies, organizations, and associations took part and had ownership in the development of a long-term strategy intended to identify (then) current and projected issues with the collection of evidence and finding solutions for those issues that would benefit the whole law enforcement community.

The law enforcement community, through the Law Enforcement Executive Forum (LEEF), a diverse group of Federal, State, local, and tribal law enforcement executive management representatives, was integral in describing to DOJ the need for the NDCAC. The LEEF developed an NDCAC Business Plan in 2010 that outlined the core functionality of the NDCAC, the role of the NDCAC EAB, and the day-to-day management of the NDCAC. The LEEF identified the NDCAC's mission "to leverage and share the collective technical knowledge and resources of the law enforcement community on issues involving real-time and stored communications and to strengthen law enforcement's relationship with industry."

The NDCAC exists to serve the current and future interests of the entire law enforcement community and it is provided advice and recommendations by the NDCAC EAB – a fifteen-member, State and local plus-one majority board composed of executive managers from across law enforcement. NDCAC EAB members' backgrounds reflect a broad range of law enforcement expertise and interests. The NDCAC EAB includes a variety of executives and officials from both large and small jurisdictions. The NDCAC EAB also includes a prosecutor from the State or local level. A core purpose of the EAB is to provide advice to the Attorney General (or his designee) and to the Director of the NDCAC that promotes public safety and

national security by advancing the NDCAC's core functions. The EAB was established under the requirements of the FACA and is limited to providing advice and recommendations to the Attorney General (or his designee) and to the Director of the NDCAC.

Knowledge Base – How the NDCAC Acquires and Grows Its Expertise

NDCAC Subject Matter Experts

The NDCAC is staffed with personnel with investigative expertise from the FBI, DEA, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and United States Marshals Service (USMS); as well as support personnel with extensive law enforcement experience at the State and local level. In addition, the NDCAC has contracted technical subject matter experts with experience in Federal, State, and local law enforcement and the communications industry (e.g., service providers, technical standards).

The NDCAC's fifty-six (56) contracted personnel include telecommunications and network engineers; technical standards and testing engineers; software developers, and systems and website administrators; technical support personnel; technical analysts and writers; and administrative support personnel.

Internal Research and Analyses

The NDCAC researches emerging communications services and technologies and assesses their respective impact on law enforcement while simultaneously building industry relationships and maintaining awareness of business and technology trends by attending key standards and industry forum meetings or conferences. The NDCAC identifies and understands new service capabilities and emerging technologies to gain insight into provider plans to assist law enforcement and help providers understand law enforcement needs.

The NDCAC analyzes communications applications and technologies to determine their respective investigative value. For example, the NDCAC delves into major communications applications to learn how they function and assess the information law enforcement may receive from a provider: what information can be provided to law enforcement and how subjects of an investigation can evade law enforcement.

The NDCAC also researches open source information to glean as much information as possible from public sources made available by various industry segments (e.g., equipment manufacturers, service providers).

Law Enforcement Subject Matter Experts

The NDCAC's ability to serve as an effective assistance center is based on its extensive collaboration with internal and external resources. The NDCAC relies, in part, on the cultivated relationships it maintains with individual subject matter experts within the law enforcement community across the Federal, State, and local law enforcement community – to gain insight into the technical impediments faced across the country. These relationships allow the NDCAC to maintain a thorough and up-to-date understanding of law enforcement concerns which in turn allow the NDCAC to tailor its support efforts.

NDCAC Programs

Outreach

The NDCAC's law enforcement and industry outreach efforts are designed to create awareness and understanding about the NDCAC and the services and tools it provides; to communicate with and engage stakeholders; and to facilitate the transparency of NDCAC operations to law enforcement and industry stakeholders and customers. To increase awareness of its capabilities, the NDCAC has hosted tours for personnel of various Joint Task Forces; law enforcement and prosecutorial representative associations and organizations; and has participated in law enforcement and industry conferences. The NDCAC also sponsors regional training to cultivate the relationship between itself and members of the law enforcement and prosecutorial communities and make them aware of the support provided by the NDCAC.

The NDCAC also strives to collaboratively establish processes with industry to identify standardized law enforcement requests (e.g., format of information responses). The NDCAC seeks out new service providers to assist them in preparing processes that facilitate responses to legal demands for the services they offer. This includes collecting and sharing best practices from other service providers and working with service providers to understand their procedures and formats of their responses. The goal is to reduce response time – recognizing that time is money to service providers; and excessive delays result in the decay of evidence for law enforcement investigators. An additional benefit of engaging the NDCAC is that service providers can leverage it to reduce some of the burden of answering the same or similar questions from many law enforcement agencies. By providing information and insight to the NDCAC for distribution to the law enforcement community, service providers can reach many agencies simultaneously.

Technology Sharing

The NDCAC provides a diverse suite of tools to the law enforcement community to assist in making available innovative solutions that address technological impediments faced by the nation's law enforcement community. The NDCAC has shared tools or provided access to databases to over 7,000 users. Examples of those tools include:

- An investigative resource and fully searchable tool that identifies cell sites/towers throughout the U.S.
- An application that provides a simple interface to process, compare and display one or more call detail reports using common data fields.
- A software application and graphical user interface designed for electronic surveillance presentation and viewing.
- A tool to read IP addresses and parse out relevant information and create a report with quick to read statistics and IP ownership information.
- A tool to categorize wireless devices by type (International Mobile Equipment Identity – IMEI).
- A tool to assist with open source research utilizing numerous social media platforms.
- A preview tool that enables investigators to safely review evidentiary data collected by them on a variety of digital media in a write protected environment.
- An intercept simulation tool to simulate the delivery of intercept data to law enforcement's collection equipment. The tool can be used by agencies to assess the

compatibility of their collection system with new technologies or new service providers; as well as for educational purposes, such as training new staff.

Training

A primary focus of the NDCAC is to provide training to the law enforcement community because law enforcement does not currently have an infrastructure to support proactive education for technical communications topics and the impacts on lawful intercept. The NDCAC develops and provides a comprehensive curriculum to educate law enforcement on new and emerging services and technologies by leveraging existing training opportunities and making them available to the law enforcement community. It develops in-house training to fill gaps in existing communication training programs.

Examples of internally-developed courses include "Modern Internet Communication Services Course" that provides students with an understanding of new communication services and technologies that enhance criminal investigative techniques and promote best practices across the law enforcement community. Students are introduced to packet data communication, data pen registers, how each impacts a criminal investigation, and how law enforcement can interpret and process legally authorized collected data. A second course, "Understanding Investigative Techniques for Modern Telecommunications," equips law enforcement with basic skills such as cellular data record analysis, geospatial mapping, and cell site analysis. A third course, "Best Practices - Collection/Seizure of Mobile Devices for Investigators," provides investigators and first responders with information related to the search and seizure of mobile devices. This course helps the investigator or first responder to identify digital evidence and take precautions to preserve evidence. The training also alerts students to the specialized and extensive analysis that may be required to review data contained on the device. Students are also provided a clear understanding of the required documentation and the potential for testimony relating to device seizure and forensic analysis. NDCAC-sponsored onsite classes have hosted 1,165 students from 426 law enforcement agencies.

The NDCAC conducts regional training across the country to expand law enforcement's understanding of the complex issues surrounding advancing communications services, technology, and devices. Regional training also allows the NDCAC to make law enforcement aware of the services and support made available through the NDCAC. The NDCAC also provides training to prosecutors to expand their understanding of the technical capabilities available to investigators and the challenges associated with today's complicated technological environment. NDCAC regional training has been provided to 1,153 students from 456 Federal, State, local, and tribal law enforcement agencies.

Examples of courses developed by other agencies and leveraged by the NDCAC for the benefit of the law enforcement community include the FBI's Project Pinpoint; the DEA's Social Media course; and two courses from the United States Secret Service – National Computer Forensics Institute (i.e., Basic Investigation of Computer and Electronic Crimes Program and Basic Mobile Device Investigation). NDCAC-leveraged classes provided by other agencies have hosted 4,376 students from 1,071 law enforcement agencies.

Technical Resources

The NDCAC provides real time support from 6:00 am to 12:00 am Eastern Standard Time (EST), Monday through Friday, to facilitate law enforcement personnel calling and talking to current and former investigators and subject matter experts. The NDCAC provides coordinated technical assistance to the law enforcement community for challenges relating to advanced communications services and technologies and assists thousands of law enforcement officers by providing valuable and actionable guidance regarding the service of legal demands, interpreting returns received from communications service providers, and the capabilities of these communications service providers. The NDCAC receives requests for and provides technical assistance on a wide variety of issues from the field ranging from point of contact and other information regarding service providers, cellular data record analysis, and data extraction. Since its foundation, the NDCAC has registered more than 12,000 clients from across the law enforcement community that can request training and access to tools.

In addition, the NDCAC maintains a secure website as an interface for the law enforcement community to access a variety of technical products and services, register for training, and access a variety of technical whitepapers on advanced communication services.

EAB's Path Forward

The NDCAC EAB recognizes the need to establish a Technology Subcommittee to provide insight and an in-depth understanding to the EAB of the technical challenges faced by the law enforcement community and how best the NDCAC could provide assistance. The primary focus of those efforts would be to further identify the technical challenges to law enforcement's lawful access to communications evidence (e.g., data at rest), electronic surveillance (e.g., data in motion), and technical location capabilities. Coupled with those responsibilities, the Technology Subcommittee would solicit information from subject matter experts with respect to the potential impacts of ongoing and proposed legislative actions. The Technology Subcommittee would examine how the NDCAC could most effectively conduct private sector interaction; and identify vital projects, tools, and training the NDCAC could undertake.

One such potential tool the Technology Subcommittee will examine is for the NDCAC to facilitate increasing the efficiency of the transactional nature of law enforcement requests for information and/or records from service providers. The EAB believes there is a need to enhance the law enforcement community's capability to interact with industry by either developing an automated mechanism to interface with service providers on multiple types of subpoenas or leveraging an existing system as a starting point for further refinement by the NDCAC. This would allow law enforcement to receive data critical to evidence collection and investigation continuity. This type of capability could also aid in the collection of statistics to further identify issues related to law enforcement's records-based requests.

Recommendation

The challenges faced by the State and local law enforcement community do not always align completely with those of its Federal partners. Jurisdictional specific issues, the types of crimes investigated, and available resources often result in nuanced differences between how law

enforcement at the State and local level can make effective use of solutions. This is particularly true with respect to statutory changes at the Federal level. The NDCAC EAB recommends the Department institute a comprehensive vetting of implications at all levels of law enforcement (i.e., Federal, State, local, and tribal) as integral to any process that pursues changes to statutes at the Federal level. The NDCAC EAB also recommends the Department ensure a thorough examination of implications at the State and local level is undertaken before mitigation strategies are instituted within Federal law enforcement and with industry partners.

Recognizing the issues presented herein are complex and deeply intertwined, the EAB recommends that its members meet with the Attorney General (or his designee) to provide further insight and clarification and to provide answers to any questions that may arise as a result of this report.